

PATENT ABSTRACTS OF JAPAN

AD

(11)Publication number : 2004-350044

(43)Date of publication of application : 09.12.2004

(51)Int.Cl.

H04L 9/08

(21)Application number : 2003-144992

(71)Applicant : TDK CORP

(22)Date of filing : 22.05.2003

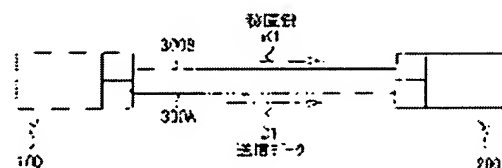
(72)Inventor : SAITO YOSHIHIRO

(54) TRANSMITTER, RECEIVER, COMMUNICATION SYSTEM, AND COMMUNICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a transmitter, a receiver, a communication system, and a communication method which enhance security of communication information.

SOLUTION: A communication device 100 and a communication device 200 transmit and receive enciphered data through transmission lines 300A and 300B. Transmission data D2 is enciphered by using a secret key K1. When the transmission line 300A is used for transmission of transmission data D1, a transmission line other than the transmission line 300A< namely, the transmission line 300B is used for delivery of the secret key K1. For example, LAN cable is used as the transmission line 300A, and a power line is used as the transmission line 300B.



LEGAL STATUS

[Date of request for examination]

31.01.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-350044

(P2004-350044A)

(43) 公開日 平成16年12月9日 (2004.12.9)

(51) Int. Cl.⁷

H04L 9/08

F I

H04L 9/00

601B

テーマコード (参考)

5J104

H04L 9/00

601E

審査請求 未請求 請求項の数 19 O L (全 21 頁)

(21) 出願番号

特願2003-144992 (P2003-144992)

(22) 出願日

平成15年5月22日 (2003.5.22)

(71) 出願人 000003067

T D K 株式会社

東京都中央区日本橋1丁目13番1号

(74) 代理人 100109656

弁理士 三反崎 泰司

(74) 代理人 100098785

弁理士 藤島 洋一郎

(72) 発明者 斉藤 義広

東京都中央区日本橋一丁目13番1号 テ

ィーディーケイ株式会社内

Fターム (参考) 5J104 EA16 EA21

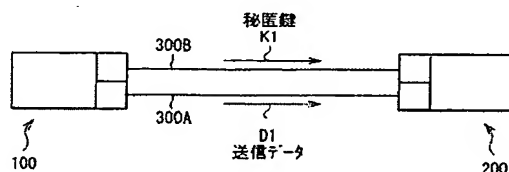
(54) 【発明の名称】 送信機および受信機、ならびに通信システムおよび通信方法

(57) 【要約】

【課題】 通信情報の秘密保護を強化することが可能な送信機および受信機、ならびに通信システムおよび通信方法を提供する。

【解決手段】 通信装置100と通信装置200は、伝送路300A、300Bを介して暗号化されたデータの送受信を行う。送信データD1は、秘匿鍵K1を使って暗号化されている。送信データD1の伝送に伝送路300Aを用いる場合には、秘匿鍵K1の受け渡しに伝送路300A以外の経路、つまり伝送路300Bを用いる。例えば、伝送路300AにはLANケーブル、伝送路300Bには電力線が適用される。

【選択図】 図3



【特許請求の範囲】

【請求項1】

複数の伝送路を利用して受信機との間で通信を行う送信機であって、
秘匿鍵を用いて秘匿化した送信データを、前記複数の伝送路のうちの1の伝送路を経由して前記受信機に送信すると共に、
前記秘匿鍵を、前記複数の伝送路のうちの他の伝送路を経由して前記受信機に送信することを特徴とする送信機。

【請求項2】

前記秘匿鍵を送信する他の伝送路として、1つの伝送路を用いることを特徴とする請求項1に記載の送信機。

10

【請求項3】

前記秘匿鍵を送信する他の伝送路として、2以上の伝送路を用い、これらの伝送路に前記秘匿鍵を分割して送信することを特徴とする請求項1に記載の送信機。

【請求項4】

前記送信データの種類もしくは量、前記受信機の種類、または、前記受信機が有する固有アドレス情報もしくはその固有アドレス情報の種類に応じて、前記複数の伝送路の中から前記送信データの送信に用いる伝送路と前記秘匿鍵の送信に用いる伝送路とを決定することを特徴とする請求項1ないし請求項4のいずれか1項に記載の送信機。

【請求項5】

装置全体の制御を行う主制御部と、
前記複数の伝送路の各々に対応して設けられると共に、それぞれが、前記主制御部から入力された前記送信データまたは前記秘匿鍵を、対応する伝送路を経由して前記受信機に送信する複数の送信制御部とを備え、
前記主制御部が、前記複数の伝送路の中から、前記送信データの送信に用いる伝送路と前記秘匿鍵の送信に用いる伝送路とを決定し、決定された各伝送路に対応する各送信制御部に前記送信データまたは前記秘匿鍵を渡すことを特徴とする請求項1ないし請求項4のいずれか1項に記載の送信機。

20

【請求項6】

前記複数の伝送路に対応して統括的に設けられ、前記送信データおよび前記秘匿鍵が供給される統括送信制御部を備え、
前記統括送信制御部が、前記複数の伝送路の中から、前記送信データの送信に用いる伝送路と前記秘匿鍵の送信に用いる伝送路とを決定することを特徴とする請求項1ないし請求項4のいずれか1項に記載の送信機。

30

【請求項7】

前記送信データが複数系統の送信データを含み、
前記複数系統のうちの1の系統の送信データが送信される伝送路を経由して、他の系統の送信データの秘匿化に用いた秘匿鍵を送信することを特徴とする請求項1ないし請求項6のいずれか1項に記載の送信機。

40

【請求項8】

前記1の伝送路と前記他の伝送路とは、互いに異なる種類の伝送路であることを特徴とする請求項1ないし請求項7のいずれか1項に記載の送信機。

【請求項9】

互いに異なる周波数帯の複数の搬送波を利用して受信機との間で通信を行う送信機であって、
秘匿鍵を用いて秘匿化した送信データを、前記複数の搬送波のうちの1の搬送波を用いて前記受信機に送信すると共に、
前記秘匿鍵を、前記複数の搬送波のうちの他の搬送波を用いて前記受信機に送信することを特徴とする送信機。

50

【請求項10】

複数の伝送路を利用して送信機との間で通信を行う受信機であって、
秘匿鍵を用いて秘匿化された送信データを、前記複数の伝送路のうちの1の伝送路を経由して前記送信機から受信すると共に、
前記秘匿鍵を、前記複数の伝送路のうちの他の伝送路を経由して前記送信機から受信することを特徴とする受信機。

【請求項11】

前記秘匿鍵を受信する他の伝送路として、1つの伝送路を用いることを特徴とする請求項10に記載の受信機。

【請求項12】

2以上の伝送路に分割されて送られてきた前記秘匿鍵を受信することを特徴とする請求項10に記載の受信機。

【請求項13】

装置全体の制御を行う主制御部と、

前記複数の伝送路の各々に対応して設けられると共に、それぞれが、対応する伝送路を経由して前記送信機から送られてきた前記送信データまたは前記秘匿鍵を受信する複数の受信制御部と

を備え、

前記主制御部が、前記複数の受信制御部から、前記送信データおよび前記秘匿鍵を受け取る

ことを特徴とする請求項10ないし請求項12のいずれか1項に記載の受信機。

【請求項14】

前記複数の伝送路に対して統括的に設けられ、前記複数の伝送路を経由して送られてきた前記送信データおよび前記秘匿鍵を受信する統括受信制御部を備えた

ことを特徴とする請求項10ないし請求項12のいずれか1項に記載の受信機。

【請求項15】

前記送信データが複数系統の送信データを含み、

前記複数系統のうちの1の系統の送信データが送られてきた伝送路を経由して、他の系統の送信データの秘匿化に用いられた秘匿鍵を受信する

ことを特徴とする請求項10ないし請求項14のいずれか1項に記載の受信機。

【請求項16】

前記1の伝送路と前記他の伝送路とは、互いに異なる種類の伝送路である

ことを特徴とする請求項10ないし請求項15のいずれか1項に記載の受信機。

【請求項17】

互いに異なる周波数帯の複数の搬送波を利用して送信機との間で通信を行う受信機であって、

秘匿鍵を用いて秘匿化され前記複数の搬送波のうちの1の搬送波を用いて前記送信機から送信された送信データを受信すると共に、

前記複数の搬送波のうちの他の搬送波を用いて前記送信機から送信された前記秘匿鍵を受信する

ことを特徴とする受信機。

【請求項18】

複数の伝送路を利用して通信を行う通信システムであって、

秘匿鍵を用いて秘匿化した送信データを前記複数の伝送路のうちの1の伝送路を経由して前記受信機に送信すると共に、前記秘匿鍵を前記複数の伝送路のうちの他の伝送路を経由して前記受信機に送信する送信機と、

秘匿鍵を用いて秘匿化された前記送信データを前記1の伝送路を経由して受信すると共に、前記秘匿鍵を前記他の伝送路を経由して受信する受信機と

を備えたことを特徴とする通信システム。

【請求項19】

10

20

30

40

50

複数の伝送路を利用して送信機と受信機との間で通信を行う通信方法であって、前記送信機は、秘匿鍵を用いて秘匿化した送信データを前記複数の伝送路のうちの1の伝送路を経由して前記受信機に送信すると共に、前記秘匿鍵を前記複数の伝送路のうちの他の伝送路を経由して前記受信機に送信し、前記受信機は、秘匿鍵を用いて秘匿化された前記送信データを前記1の伝送路を経由して受信すると共に、前記秘匿鍵を前記他の伝送路を経由して受信することを特徴とする通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、秘匿情報の伝達、特に共通鍵暗号を用いる秘匿データの通信に適用される送信機および受信機、ならびに通信システムおよび通信方法に関する。

【0002】

【従来の技術】

通信ネットワークは、インターネットの普及等によって高速・大容量化が急速に進んでおり、一方ではユビキタスを志向した通信システムが電力線や無線などを利用して構築されつつある。こうしたネットワーク環境の発達に伴って情報の流通経路も変化し、現在では、メールやコンテンツ配信のほか、インターネットショッピング、インターネットバンキング、インターネット株取引、電子調達、電子申請、病院情報ネットワーク、企業内認証（電子社員証など）などが行われるようになってきている。

【0003】

これらの活動を、盗聴やなりすましなどが容易なインターネット上でも安全に実行できるようにするためには、セキュリティ基盤の整備が重要である。簡易なセキュリティ対策としては、データファイルにファイルを開くためのパスワードを設定すること等が広く行われており、機密情報のやりとりには、暗号化技術が用いられている。

【0004】

例えば、共通鍵暗号方式では、送信者は、秘密にしたいデータを鍵（ある特定の変換規則）を用いて暗号化し、秘匿状態としたデータと暗号化に用いた鍵とを受信者宛てに送信する。受信者は、秘匿データと鍵を受信すると、データを鍵を用いて復号し、元の平文を得るようになっている。

【0005】

よって、鍵がなければデータの復号は困難であることから、通信内容は第三者に対し秘匿されることになる。こうした暗号化による情報セキュリティ機能をより高める技術としては、秘匿化するデータを単独では意味のない複数のデータに分割し、それぞれを複数の通信路に振り分けて伝送するようにするものが挙げられる（特許文献1参照）。これにより、秘匿情報全体の盗聴を困難とし、たとえデータの一部が盗聴されても解読はできないようにすることが可能となる。

【0006】

【特許文献1】

特開2000-115162号公報

【0007】

【発明が解決しようとする課題】

しかしながら、共通鍵暗号方式では、従来より「鍵の受け渡しかた」が問題となっていた。すなわち、盗聴などによって鍵を参照した第三者にとっては、秘匿化データを参照するのは容易であるため、いかにして通信途中で鍵を盗まれないようにするかが、データ漏洩を防止する上での焦点となっていた。

【0008】

本発明はかかる問題点に鑑みてなされたもので、その目的は、通信情報の秘密保護を強化することが可能な送信機および受信機、ならびに通信システムおよび通信方法を提供することにある。

10

20

30

40

50

【0009】

【課題を解決するための手段】

本発明の第1の観点に係る送信機は、複数の伝送路を利用して受信機との間で通信を行う送信機であって、秘匿鍵を用いて秘匿化した送信データを複数の伝送路のうちの1の伝送路を経由して受信機に送信すると共に、秘匿鍵を複数の伝送路のうちの他の伝送路を経由して受信機に送信するものである。

【0010】

本発明における「伝送路」には、物理的な線路状媒体だけでなく、無線通信路も含まれている。物理的な線路状媒体としては、例えばイーサネット(R)などに適用されるLANケーブルや、Home PNA (Home Phoneline Networking Alliance) 等で適用される電話回線、光ファイバケーブル、ケーブルテレビ (CATV) のケーブル、電力線等がある。また、ここでのいう無線通信路とは、有体の線路を用いずに、電波や光を用いて構成される空間伝送路をいい、例えば無線LAN、ブルートゥース(R)、IR (赤外光) 通信等が含まれる。また、本発明における「秘匿鍵」には、データの内容自体を暗号化するための暗号化キーの他、データファイルの保存時に設定されるパスワードのような、データファイルを開くための単なる解除キーも含まれ、「秘匿化」ということは、送信データを秘匿鍵を用いないと解読できない状態にすることを指している。

【0011】

本発明の第1の観点に係る送信機では、秘匿鍵が、この秘匿鍵を使って秘匿化したデータを送出する伝送路とは異なる伝送路に送出される。この送信機においては、送信データの送信に用いる伝送路と秘匿鍵の送信に用いる伝送路がともに、利用可能な複数の伝送路の中から決定される。データ送信用としては常に1の伝送路が選択されるが、秘匿鍵の送信には、例えば、この1の伝送路を除く複数の伝送路のなかから選んだ1つの伝送路だけを用いるようにしてよい。また、秘匿鍵を分割し、その分割データを2以上の伝送路の各々に送信するようにしてもよい。また、伝送路を2つとしておき、一方で送信データを伝送し、他方で秘匿鍵を伝送するようにすることもできる。

【0012】

なお、こうした場合に、送信データおよび秘匿鍵を伝送する各伝送路は、送信データの種類もしくは量、受信機の種類、または、受信機が有する固有アドレス情報もしくはその固有アドレス情報の種類に応じて決定されることが好ましい。ここでのいう「送信データの種類」とは、主としてアプリケーションソフトウェアによって定まるデータ形式を指す。例えば、ワードデータ、エクセルデータ、CADデータ (ベクトルデータ)、画像データにおけるビットマップ形式などである。「送信データの量」とは、送信データのサイズ、具体的にはファイルサイズ等である。また、「受信機の種類」とは、一般的なクライアントPC (PC; パーソナルコンピュータ)、サーバPCや、プリンタサーバ、データベースサーバ、通信サーバなど、それぞれの装置に予定されている機能や役割の種類のことをいう。さらに、「受信機が有する固有アドレス情報」とは、個々の装置を識別するために予め装置ごとに付与されている識別情報であり、例えば、TCP/IP (Transmission Control Protocol / Internet Protocol) で用いられるIPアドレスやMACアドレス (Media Access Control Address) 等がある。「固有アドレス情報の種類」とは、固有アドレス情報がどのようなルールに則って (あるいは、どのような範囲で) 規定されているかによる区分である。例えば、TCP/IPを例にとると、グローバルアドレスか、ローカルアドレスの区別がこれにあたる。

【0013】

この送信機は、具体的には、装置全体の制御を行う主制御部と、複数の伝送路の各々に対応して設けられると共に、それぞれが主制御部から入力された送信データまたは秘匿鍵に対応する伝送路を経由して受信機に送信する複数の送信制御部とを備え、主制御部が、複数の伝送路の中から送信データの送信に用いる伝送路と秘匿鍵の送信に用いる伝送路とを

10

20

30

40

50

決定し、決定された各伝送路に対応する各送信制御部に送信データまたは秘匿鍵を渡すように構成することができる。ここでいう「主制御部」とは、送信機の各部を統括制御する部分を指す。例えば、コンピュータであれば、OSが常駐すると共にこのOSを機能させる機能をもったメインCPUを中心とした部分である。また、「送信制御部」は、例えばNIC(Network Interface Card)のように、伝送路と主制御部の間にあって、両者間をインタフェース接続する部分をいう。

【0014】

そのほか、複数の伝送路に対して統括的に設けられ、送信データおよび秘匿鍵が供給される統括送信制御部を備え、統括送信制御部が、複数の伝送路の中から、送信データの送信に用いる伝送路と秘匿鍵の送信に用いる伝送路とを決定するように構成することもできる。なお、本発明における「複数の伝送路に対して統括的に」とは、複数の伝送路のすべてに接続され、かつ、これらすべての伝送路に対応可能になっている状態を意味している。

【0015】

さらに、送信データが複数系統の送信データを含んでいる場合には、複数系統のうちの1の系統の送信データが送信される伝送路を経由して、他の系統の送信データの秘匿化に用いた秘匿鍵を送信するようにしてもよい。この「複数系統の送信データ」とは、出所(ソース)や生成過程・処理過程等を共通として順序立てられた、統一性のある一連のデータ群が複数あることを意味している。なお、各データ群間でのデータの種類や形式の異同は問わない。

【0016】

また、送信データの送信に用いる1の伝送路と、この送信データの秘匿化に用いられた秘匿鍵の送信に用いる他の伝送路とは、盗聴を困難にすることなどから、互いに異なる種類の伝送路であることが好ましい。

【0017】

本発明の第2の観点に係る送信機は、互いに異なる周波数帯の複数の搬送波を利用して受信機との間で通信を行う送信機であって、秘匿鍵を用いて秘匿化した送信データを複数の搬送波のうちの1の搬送波を用いて受信機に送信すると共に、秘匿鍵を複数の搬送波のうちの他の搬送波を用いて受信機に送信するものである。なお、本発明において言う「互いに異なる周波数帯」とは、互いの周波数帯が完全に分離している場合の他、帯域の一部がオーバーラップしている場合も含んでいる。また、「搬送波を利用して」というのは、主として、搬送波によって送信データを変調することを指している。この第2の観点に係る送信機では、秘匿鍵は、(1)この秘匿鍵を使って秘匿化したデータとは、変調方式は同じだが異なった伝送帯域が用いられる場合と、(2)秘匿化したデータとは異なる変調方式に基づいて変調される場合とがある。その結果、送信データと秘匿鍵とは、互いに異なる伝送経路で伝送されることになる。

【0018】

本発明の第1の観点に係る受信機は、本発明の第1の観点に係る送信機との間で通信を行う受信機である。すなわち、秘匿鍵を用いて秘匿化された送信データを、複数の伝送路のうちの1の伝送路を経由して送信機から受信すると共に、秘匿鍵を、複数の伝送路のうちの他の伝送路を経由して送信機から受信するものである。

【0019】

この受信機では、利用する伝送路は送信機側と対応している必要がある。すなわち、秘匿鍵は、この秘匿鍵を使って秘匿化したデータが送られてくる伝送路とは異なる伝送路から受信される。

【0020】

秘匿鍵の受信に用いる伝送路は、複数から選択した1の伝送路である場合や、分割された秘匿鍵の各分割データが送られてくる2以上の伝送路である場合がある。また、2つの伝送路のうち、送信データ用ではないもう一方の伝送路としてもよい。受信機の具体的構成としては、例えば、装置全体の制御を行う主制御部と、複数の伝送路の各々に対応して設けられると共に、それぞれが送信機から送られてきた送信データまたは秘匿鍵に対応する

10

20

30

40

50

伝送路を経由して受信する複数の受信制御部とを備え、主制御部が、複数の受信制御部から送信データおよび秘匿鍵を受け取るようにすることができる。なお、この場合の「主制御部」、「受信制御部」の定義は、上記本発明の送信機における「主制御部」、「送信制御部」の定義と同様である。

【0021】

また、この受信機は、複数の伝送路に対応して統括的に設けられ、複数の伝送路を経由して送られてきた送信データおよび秘匿鍵を受信する統括受信制御部を備えるようにしてもよい。さらに、送信データが複数系統の送信データを含んでいる場合に、複数系統のうちの1の系統の送信データが送られてきた伝送路から、他の系統の送信データの秘匿化に用いられた秘匿鍵を受信するようにしてもよい。また、送信データが送られてくる1の伝送路と、この送信データの秘匿化に用いられた秘匿鍵を受信する他の伝送路とは、互いに異なる種類の伝送路であることが好ましい。

10

【0022】

本発明の第2の観点に係る受信機は、本発明の第2の観点に係る送信機との間で通信を行う受信機であり、秘匿鍵を用いて秘匿化され、複数の搬送波のうちの1の搬送波を用いて送信機から送信された送信データを受信すると共に、複数の搬送波のうちの他の搬送波を用いて送信機から送信された秘匿鍵を受信するものである。この第2の観点に係る受信機では、秘匿鍵は、秘匿化したデータの伝送帯域とは異なる帯域において受信される。

【0023】

本発明による通信システムは、複数の伝送路を利用して通信を行う通信システムであって、秘匿鍵を用いて秘匿化した送信データを複数の伝送路のうちの1の伝送路を経由して受信機に送信すると共に、秘匿鍵を複数の伝送路のうちの他の伝送路を経由して受信機に送信する送信機と、秘匿鍵を用いて秘匿化された送信データを1の伝送路を経由して受信すると共に、秘匿鍵を他の伝送路を経由して受信する受信機とを備えたものである。

20

【0024】

本発明による通信方法は、複数の伝送路を利用して送信機と受信機との間で通信を行う通信方法であって、送信機は、秘匿鍵を用いて秘匿化した送信データを複数の伝送路のうちの1の伝送路を経由して受信機に送信すると共に、秘匿鍵を複数の伝送路のうちの他の伝送路を経由して受信機に送信し、受信機は、秘匿鍵を用いて秘匿化された送信データを1の伝送路を経由して受信すると共に、秘匿鍵を他の伝送路を経由して受信するものである。

30

【0025】

本発明による通信システムおよび通信方法では、秘匿鍵と、この秘匿鍵を使って秘匿化したデータとは、互いに異なる伝送路を介して送受信される。

【0026】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して詳細に説明する。

【0027】

〔第1の実施の形態〕

図1は、本発明の第1の実施の形態に係る通信システムの基本構成を表している。この通信システムは、ホームネットワークを想定しており、通信装置100と通信装置200とが伝送路300(300A, 300B)を介して相互に送受信を行うようになっている。伝送路300にはLANケーブルを用いるのが一般的であるが、そのほか電話回線, CATVケーブル, 電力線などの任意の伝送媒体を用いることができる。ここでは、最も基本的な態様として、通信装置100と通信装置200が、伝送路300A, 300Bの2本で接続されている場合について説明する。

40

【0028】

ただし、このように通信網を2重に敷設するようなことは、一般家庭に限らずとも通常の使用では考えにくい。そこで、まず伝送路300Aを、既設あるいは新設するイーサネット(R)ケーブルとし、伝送路300Bには、別の既設媒体として電力線を利用するよう

50

にしている。こうした線路選択は最も現実的であり、比較的簡易にシステムを構築できる。なお、イーサネット(R)に適用されるケーブルとしては、UTPケーブル(Unshielded Twisted Pair Cable)、同軸ケーブル、光ファイバなどがある。電力線による通信システムは、既設の電力線が媒体であることから低コストであり、電気コンセントで接続できるため、ほとんどの部屋で場所を選ばず、簡便に利用できるという利点を持ち、米国では既に伝送速度14Mbpsで標準化されている。また、無線通信では、コンクリート構造、鉄筋構造、土壁などの建造物、さらには室内の人間や什器等によって電波が遮断され、通信状態が不安定化する傾向があるが、電力線通信は、こうした要因による通信状態の劣化が少ないと考えられる点でも有利である。

【0029】

通信装置100は、本体部10と、本体部10と伝送路300A、300Bの各間にあって、それぞれの間をインタフェース接続する通信制御部11A、11Bとを備えている。通信装置200も、本体部20、通信制御部21A、21Bを備えている。本体部10、本体部20は、例えばPCやワークステーション等であり、その場合の通信制御部11A、11Bないし通信制御部21A、21Bは、モデムやNICの類、すなわちデータ回線終端装置(Data Circuit terminating Equipment: DCE)に相当する。NICは、PC等を伝送路(一般的にはLAN)に接続するため、その拡張スロットに装着されるインターフェイス機器である。NICには、ISA、PCIなどの拡張バスの種類や通信方式によってイーサネット(R)・アダプタ、100BASE-T/100VG-AnyLANアダプタ、トークンリング・アダプタ、FDDI(Fiber Distributed Data Interface)アダプタなどがある。ここでは、伝送路300A(イーサネット(R)ケーブル)に接続される通信制御部11A、通信制御部21AがNIC、伝送路300B(電力線)に接続される通信制御部11B、21Bが電力線用モデムとなっている。

【0030】

図2は、通信装置100の構成を表している。なお、通信装置200は、これに対応した構成となっているため、ここでは説明を省略する。

【0031】

本体部10は、装置全体の制御を行うメインCPU1を中心として、秘匿化部2、復号部3、メインCPU1と通信制御部11A、11Bの間のデータ入出力を行うI/O部4A、4B、さらには図示しないメモリ等を備えたものである。暗号化部2は、送信するデータを暗号化することによって、秘匿鍵を用いないと解読できない状態にするものであり、暗号化したデータおよび用いた鍵をメインCPU1に出力するようになっている。また、復号部3は、メインCPU1から暗号データと鍵を受け取って復号するようになっている。メインCPU1は、(1)暗号化部2から入力される送信用の暗号データと、その暗号化に用いた鍵とを、通信制御部11A、通信制御部11Bに対して振り分けて出力する機能と、(2)受信されてくる暗号データ、暗号化に用いた鍵を、復号化部3に送出する機能を有している。

【0032】

通信制御部11Aは、本体部10-伝送路300Aの間のインタフェース機能を有しており、I/O部5A、CPU6A、RAM7A、およびイーサネット(R)物理層機能部(physical layer: PHY)8Aを備えている。イーサネット(R)物理層機能部8Aは、ビットデータを符号化し、伝送媒体に適した信号形式に変換するといった通常の物理層を含み、さらに媒体へのアクセスを制御する、いわゆるMAC(Media Access Control)処理も階層的に行うようになっている。このイーサネット(R)物理層機能部8Aには、LANポートを介してLANケーブル(伝送路300A)が接続されている。

【0033】

一方、通信制御部11Bは、本体部10-伝送路300Bの間のインタフェース機能を有しており、I/O部5B、CPU6B、RAM7B、およびAC用物理層機能部8Bを備

10

20

30

40

50

えている。ここで、AC用物理層機能部8Bはイーサネット(R)物理層機能部8Aに対応させて便宜的に設定したものであり、MAC処理を行うMAC副層および物理層に対応する。この場合の物理層は、FDM(Frequency Division Multiplex: 周波数分割多重)もしくはOFDM(Orthogonal Frequency Division Multiplex: 直交周波数分割多重)などの変調方式によりシリアルビットストリームをAC伝送用帯域の電気信号に変換するものである。このようなAC用物理層機能部8Bには、コンセントを介して電力線(伝送路300B)が接続されている。

【0034】

なお、本明細書の以下の説明では、通信制御部がデータを本体部から伝送路へと送出する際に行う処理をまとめて変調といい、伝送路から本体部へ取り込む際に行う、変調とは逆の処理を復調ということにする。また、本実施の形態においては、通信装置100、200が本発明の「送信機」および「受信機」の一具体例に対応している。さらに、本体部10、20のメインCPUが本発明の「主制御部」に、通信制御部11A、11B、通信制御部21A、21Bのそれぞれが本発明の「送信制御部」および「受信制御部」の一具体例に対応している。

【0035】

次に、この通信システムの動作について説明する。

【0036】

ここでは、一例として、秘匿化データを通信装置100から通信装置200に送信する場合について説明する。この通信システムの基本動作は、図3に示したように、暗号化された送信データD1を伝送路300Aを使って送受するとき、その秘匿鍵K1の受け渡しには、伝送路300Aとは異なる経路、つまり伝送路300Bを用いるというものである。図4は、そうした動作の詳細を示すフローチャートであり、図5は、通信装置100、200の間の応答過程を示すタイミングチャートである。

【0037】

まず、通信装置100の本体部10において、送信しようとするデータD1を暗号化部2が暗号化する。ここで用いられる暗号化方式は、例えばDES(Data Encryption Standard)などである。秘匿鍵K1は、繰り返し用いられるように予め定められていても構わないが、ここでは、データの暗号化の度に新たに生成されるものとする。こうして、秘匿鍵K1が生成されると共に、送信データD1が暗号化される(ステップS1)。暗号化部2は、送信データD1、秘匿鍵K1の双方をメインCPU1に出力する。

【0038】

〈データの振り分け〉

メインCPU1は、入力された送信データD1、秘匿鍵K1を、伝送路300A、300B(直接には通信制御部11A、11B)に向けて振り分ける(ステップS2)。この振り分けかたは、システムの状況に応じていろいろなやり方を考えることができるが、例えば、伝送するデータのサイズにあわせて伝送路300を選ぶとよい。ここでは、伝送路300Aのほうが伝送路300Bよりも高速で伝送容量も大きいことから、送信データD1を伝送路300Aに接続された側の経路に送出し、それほどサイズが大きくなることが想定される秘匿鍵K1を伝送路300Bの側の経路に送出するようにしている。

【0039】

メインCPU1から送出された送信データD1は、I/O部4Aを介して通信制御部11Aに入力され(ステップS3)、一方の秘匿鍵K1は、I/O部4Bを介して通信制御部11Bに入力される(ステップS6)。

【0040】

〈変調〉

通信制御部11Aでは、送信データD1が、I/O部5Aを介してCPU6Aに入力される。CPU6Aは、RAM7Aを適宜利用しつつ通信に必要なTCP、IP等のヘッダを

10

20

30

40

50

送信データD1に付加し、さらにイーサネット(R)物理層機能部8Aに送出する。イーサネット(R)物理層機能部8Aは、送信データD1のMACフレームを生成し、さらに符号化などを経て、伝送路300A(イーサネット(R)ケーブル)に対応する形式の信号にまで変換する。このようにして、送信データD1は通信制御部11Aにて変調され(ステップS4)、伝送路300Aに送出される(ステップS5)。

【0041】

一方、通信制御部11Bでは、秘匿鍵K1が、通信制御部11Aにおける送信データD1と同様に、伝送路300B(電力線)に適応する信号形式にまで変調される(ステップS7)。そのうち、この秘匿鍵K1は、伝送路300Bに送出される(ステップS8)。

10

【0042】

この場合、伝送路300A、300Bにおけるデータ送受信の具体的状況は、例えば図5のように表される。まず、伝送路300Bの上を、通信装置100から通信装置200へ秘匿鍵K1が送信される。通信装置200は、秘匿鍵K1を受け取ると、伝送路300Bを使って通信装置100へ受信返答を送る。通信装置100は、この受信返答を確認した後に、今度は伝送路300Aを使って通信装置200に送信データD1を送出する。通信装置200は、送信データD1を受け取ると、伝送路300Aを使って通信装置100へ受信返答を送る。この送信データD1送出の過程は、例えば送信データD1のフレームごとに繰り返し行われる。通信装置100は、送信データをすべて送った後、通信装置200からの受信返答を受けると、最後に通信装置200に対してデータ・エンド信号を送出する。

20

【0043】

なお、図6は、以上の様子をデータフローブロックで表したものである(送信のみ、受信返答は省略)。伝送路300上における送信データD1、秘匿鍵K1は、図示したように、前述の通信制御部11A、11Bの処理によってヘッダが付加されたフレームの状態である。なお、ここでは、秘匿鍵K1を送信データD1よりも先に伝送するようにしているが、これら秘匿鍵K1、送信データD1が受信側の通信装置200において対のデータであることが認識されるのであればよく、データの送出順はどのようなものであっても構わない。

【0044】

このように、送信データD1と秘匿鍵K1を別々の経路で伝送するようにすると、両方がともに傍受されるおそれが減る。仮に、伝送路300Aにおいて送信データD1が漏洩したとしても、秘匿鍵K1がなければ、その解読は非常に困難である。逆に、伝送路300Bが傍受されても、秘匿鍵K1だけしか参照されることはなく、送信データD1そのものは無事である。よって、送信データD1、秘匿鍵K1の両方を不正に入手するには、伝送路300A、300Bの双方で傍受するしかなく、従来のように同一の線路上に送信データと鍵を伝送する場合に比べ、データ漏洩のリスクが低減される。特に、ここでは伝送路300Aと伝送路300Bは異なる種類の線路であり、両方の傍受にはより手間がかかるようになっているため、漏洩リスク軽減のうえで好ましい。

30

【0045】

次に、伝送路300Aに送出された送信データD1は、通信装置200の通信制御部21Aに入力され(ステップS9)、伝送路300Bに送出された秘匿鍵K1は通信制御部21Bに入力される(ステップS11)。

40

【0046】

〈復調〉

送信データD1は、通信制御部21Aにて、通信制御部11Aで施された過程とは逆の過程を辿ることにより、復調される(ステップS10)。ただし、この時点では、送信データD1はまだ暗号化された状態にある。一方、秘匿鍵K1もまた同様に、通信制御部21Bにて復調される(ステップS12)。

【0047】

次いで、これら送信データD1、秘匿鍵K1は共に、本体部20に入力され、メインCP

50

U1を介して復号部3に入力される(ステップS13)。復号部3では、秘匿鍵K1を用いて送信データD1が解読される(ステップS14)。こうして、通信装置200において送信データD1の平文が入手される。

【0048】

なお、以上は、通信装置100から通信装置200へデータを送信する場合について説明したが、通信装置200から通信装置100へデータを送信する場合も同様に行うことができる。すなわち、両者間では、伝送路300Aでデータを伝送し、伝送路300Bで秘匿鍵を伝送することにより送受信が行われる。

【0049】

このように本実施の形態では、2つの伝送路300A、300Bのそれぞれに、暗号化した送信データD1と暗号化に用いた秘匿鍵K1を別々に伝送するようにしたので、両方がともに傍受されるおそれが減り、データ漏洩のリスクを軽減することができる。

10

【0050】

また、ここでは、伝送路300Aと伝送路300Bは種類の異なる媒体であることから、双方の傍受をさらに困難としてより秘匿データの安全性を高めることができるほか、同一の媒体をわざわざ2重に敷設するという手間をかけず、適宜に使用可能な媒体を利用して構築できるという利点がある。

【0051】

次に、上記第1の実施の形態の変形例について説明する。

【0052】

20

〔変形例1〕

第1の実施の形態では、送信データは伝送路300A、秘匿鍵は伝送路300Bに振り分けて伝送するようにしたが、このように伝送路300A、300Bの役割を固定せず、状況に応じて送信データ、秘匿鍵を伝送路300A、300Bのそれぞれが割り当てられるようにすることができる。例えば、図7のように、第1の実施の形態と同様の通信システムにおいて、送信データD1については伝送路300Aに送信データD1、伝送路300Bにその秘匿鍵K1を送出する。しかし、送信データD2については、逆に伝送路300Aに秘匿鍵K2、伝送路300Bに送信データD2を送出する場合である。

【0053】

図8は、第1の変形例におけるデータ通信動作のタイミングチャートである。同図の場合、まず送信データD1(および秘匿鍵K1)の送信を行った後、送信データD2(および秘匿鍵K2)の送信を行うようになっている。送信データD2では、送信データD1の送信時とは振り分け先の伝送路300が異なるだけで、秘匿鍵K2の生成から復号までの一連の過程は同様に行われる。

30

【0054】

また、図9は、この第1の変形例におけるデータフローブロックの例を示している。この場合には、図8とは異なり、送信データD1と送信データD2の送信がほぼ同時に行われている。これまでの方式では、第1の実施の形態にて前出のデータフロー(図6)からわかるように、秘匿鍵K1を伝送路300Bに伝送しているときには、伝送路300Aは利用されていない。次いで、送信データD1を伝送路300Aに伝送しているときには、伝送路300Bが空いている。そこで、この例では、送信データD1、D2のデータフローがモザイク状となる格好にして、2種類のデータの通信をほぼ同時に行っている。送信データおよび秘匿鍵は、振り分けられた後はあたかも互いに独立したデータのように決められた伝送路300を伝送され、通信装置200において送信データと秘匿鍵が対照される。

40

【0055】

こうした送信データに応じた伝送路300A、300Bの使い分けは、例えば、以下のようデータ振り分け条件に基づいて行われる。

▲1▼送信データの種類。例えば、ワードデータ、エクセルデータ、CADデータ(ベクトルデータ)、ビットマップ形式の画像データなどのデータ形式に応じて、伝送路300

50

A, 300Bのいずれかに送信データを振り分け、残ったもう一方の伝送路に秘匿鍵を振り分ける。通常、CADデータや画像データは文書に比べてサイズが大きいので、より伝送速度が大きい伝送路に優先的に送出することが考えられる。なお、インターネットのホームページなど、1つのデータファイルに画像と文章が存在する場合には、一旦、画像ファイルと文書ファイルに分割し、それぞれについて伝送路を決定することもできる。その場合、各分割データを1つの送信データとみたと、それぞれについて暗号化処理を施し、対応する秘匿鍵を生成するようにしてもよい。

【0056】

▲2▼受信側の装置の種類。通信装置には、一般的なクライアントPCやサーバPC、プリンタサーバ、データベースサーバ、通信サーバ等があるが、そうした装置の種類に応じてデータを振り分ける。さらには、そのうち機密性が高い装置に対してのみ、こうした2重の伝送路による通信を行うように制御するようにしてもよい。

10

【0057】

▲3▼受信側の個々の装置が有する固有アドレス情報。例えばIPアドレスやMACアドレスを参照することにより、受信側の装置のそれぞれに対応させてデータの振り分け方を決めることができる。

【0058】

▲4▼受信側装置のIPアドレスの種類。つまり、グローバルアドレスか、ローカルアドレスかを基準にして行うこともできる。この区別は、一般家庭であれば受信相手が屋外（インターネットを通じて接続）であるか、屋内（LANで接続）であるかということになる。

20

【0059】

▲5▼伝送路300A, 300Bの混み具合。例えば、送信前に伝送路300Aの混み具合を判断し、ある程度以上混んでいる場合には送信データは伝送路300Bに送出するようにする。

【0060】

〔変形例2〕

図10は、第2の変形例に係る通信システムの構成図である。第1の実施の形態では、通信装置100, 200は伝送路ごとに通信制御部を備えるようにしたが、本変形例では、通信装置101, 201はそれぞれ1つの通信制御部11, 21を備え、通信制御部11, 21が伝送路300A, 300Bの双方に接続されている。これら通信制御部11, 21は、単にデータを出力するためのインターフェイス機能を果たすだけではなく、送信の際には暗号化された送信データとその秘匿鍵を伝送路300A, 300Bのいずれに送出するかを判断する機能を有している。なお、通信装置101と通信装置201とは、対応関係にある構成要素によって対称な構成となっているものとする。

30

【0061】

次に、図11を参照して通信装置101の構成について説明する。本体部30は、第1の実施の形態における本体部10と同様の構成要素からなる（詳細は図示せず）。ただし、本体部10のメインCPU1に与えられていた「送信データ、秘匿鍵を伝送路に振り分ける」機能は、本体部30のメインCPUにはない。よって、本体部30は、通信制御部11との間では暗号化した送信データおよび秘匿鍵のやり取りを行うだけである。

40

【0062】

一方、通信制御部11は、通信制御部11A, 11Bを統合したようになっており、伝送路300A, 300Bに対して総括的に設けられている。通信制御部11は、I/O部5, CPU6, RAM7, イーサネット(R)物理層機能部8AおよびAC用物理層機能部8Bを備えており、ここでは、CPU6が「送信データ、秘匿鍵を伝送路に振り分ける」機能を有している。すなわち、データ送信時には、本体部30からI/O部5を通じて送信データとその秘匿鍵が入力され、CPU6は、これらを伝送路300A, 300Bごとに振り分けて、それぞれイーサネット(R)物理層機能部8A, AC用物理層機能部8Bに入力する。送信データと秘匿鍵は、イーサネット(R)物理層機能部8A, AC用物

50

理層機能部 8 B を介して、それぞれ伝送路 3 0 0 A, 3 0 0 B に送出される。また、この通信制御部 1 1 は、伝送路 3 0 0 A, 3 0 0 B のそれぞれを経由して送られてくる送信データおよび秘匿鍵の両方とも受信するようになっている。

【 0 0 6 3 】

以上の通信装置 1 0 1 の本体部 3 0、通信制御部 1 1 の作用構成は、通信装置 2 0 1 の本体部 4 0、通信制御部 2 1 についても同様である。なお、この第 2 の変形例においては、CPU 6 が本発明の「総括送信制御部」および「総括受信制御部」に対応し、通信制御部 1 1、2 1 が本発明の「送信機」および「受信機」に対応する一具体例となっている。

【 0 0 6 4 】

このように第 2 の変形例では、通信制御部 1 1、2 1 が、本体部 3 0、4 0 と伝送路 3 0 0 とのインターフェイス機能に加え、「送信データと秘匿鍵の振り分け」機能を備えるようにしたので、本体部 3 0、4 0 には、旧来の PC 等をそのまま適用することができる。すなわち、第 1 の実施の形態の通信装置 1 0 0、2 0 0 では、通常用いられる PC カードを伝送路 3 0 0 ごとに設ければよい代わりに、本体部 1 0、2 0 のメイン CPU 1 にデータ振り分け機能を追加設定しなければならない。これに対し、本変形例では、データ振り分け機能を有し、複数の伝送路に接続可能な 1 枚の PC カードを装着するだけで済むために、システムをより簡便に構築できると考えられる。

【 0 0 6 5 】

〔第 2 の実施の形態〕

図 1 2 は、第 2 の実施の形態に係る通信システムの構成を表したものである。この通信システムは、伝送路 3 0 0 B (電力線) を伝送路 3 0 0 C (無線) に替えたことに関したことを除けば第 1 の実施の形態のシステムと同様に構成されている。なお、以下の実施の形態においては、それより先に説明した実施の形態を受けて説明するものとし、同様の構成要素については同一の符号を付し、説明を適宜省略するものとする。

【 0 0 6 6 】

伝送路 3 0 0 C は、無線 LAN, ブルートゥース (R), IR (赤外光) 通信などの無線通信による伝送経路である。これら無線通信では、装置の設置場所を選ばず、屋外・屋内で、また移動しながら送受信を行うことができ、物理的線路の敷設が不要なために極めて簡単に構築できる。そのため、インターネットの中継スポットとして、また、ネット家電や携帯端末を結ぶホームネットワーク等に利用されつつある。

【 0 0 6 7 】

この伝送路 3 0 0 C は、一端が通信装置 1 0 2 の通信制御部 1 1 C に接続され、他端が通信装置 2 0 2 の通信制御部 2 1 C に接続されている。通信制御部 1 1 C, 2 1 C はともに、無線 LAN カードもしくはブルートゥース (R) PC カード等であり、図 1 3 のように構成されている。これらは、I/O 部 5 C, CPU 6 C, RAM 7 C および無線用物理層機能部 8 C を備えている。このうち、無線用物理層機能部 8 C が、OFDM 等の方式によって、データをそれぞれの規格に応じた電波もしくは光に変換し出力するようになっている。

【 0 0 6 8 】

したがって、本実施の形態における通信システムの動作は、第 1 の実施の形態における通信制御部 1 1 B の動作を通信制御部 1 1 C が、通信制御部 2 1 B の動作を通信制御部 2 1 C がそれぞれ行うものとすれば説明できる。また、本実施の形態におけるシステムに上記変形例の伝送手法を適用することも可能である。

【 0 0 6 9 】

このように本実施の形態における通信システムは、2 つの伝送路 3 0 0 A, 3 0 0 C のそれぞれに暗号化した送信データと暗号化に用いた秘匿鍵を振り分けて伝送するようにしたので、第 1 の実施の形態と同様の効果を奏する。また、無線通信は一般に有線通信に比べてセキュリティが脆弱であることが知られているが、伝送路 3 0 0 C だけでなく伝送路 3 0 0 A を利用したこの手法によって脆弱性を補完することができる。

【 0 0 7 0 】

10

20

30

40

〔第3の実施の形態〕

図14は、第3の実施の形態に係る通信システムの構成を表したものである。この通信システムは、第1および第2の実施の形態の各システムを合体したようになっている。すなわち、本体部50、通信制御部11A～11Cを備えた通信装置103と、本体部60、通信制御部21A～21Cを備えた通信装置203とが、伝送路300（300A、300B、300C）を介して相互に送受信を行うようになっている。通信制御部11A～11C、21A～21Cおよび伝送路300A～300Cについては、第1および第2の実施の形態で説明した通りである。ただし、この場合には伝送路が3つであることから、本体部50、60は、送信データと秘匿鍵の振り分け方が本体部10、20とは異なる。

【0071】

本体部50、60のメインCPU1では、まず送信データを伝送路300A～300Cのいずれに送出するかを決める必要がある。これには、第1の実施の形態におけるデータの振り分けかたを応用することができる。例えば、送信データのファイルサイズが大きければ、送信データ用には伝送路300A（LANケーブル）を選択するなど、各伝送路300の伝送特性や送信データのサイズを考慮するようにしてもよいし、第1の変形例にて前述した▲1▼～▲5▼の基準を適用してもよい。

【0072】

秘匿鍵については、この場合、（1）送信データを送出する伝送路を除き、残った2つの伝送路のいずれかに送出するか、（2）2つに分割し、各分割データを残った2つの伝送路に送出するかの2種類の伝送方法が考えられる。（1）の方法では、送信データの場合と同様に伝送路の選択を行うとよい。秘匿鍵の場合には、選択基準として最も優先順位が高いのは、秘匿性がより高い伝送路であると考えられる。（2）の方法では、例えば、単に秘匿鍵のコードを伝送路の数に分割することもできるし、所定の規則に基づいて秘匿鍵の各ビットを分配し、それぞれが単独では意味を成さないビット列に変換することもできる。このように秘匿鍵を分割して送信すると、秘匿鍵の不正入手が一層困難となる。

【0073】

例えば、通信装置103が送信データD1を送出する場合についてみる。暗号化した送信データD1を伝送路300Aに送出するとすれば、秘匿鍵K1は、（1）伝送路300Bまたは伝送路300Cのいずれか一方に送出する（2）2つに分割し、分割データをそれぞれ伝送路300B、300Cに送出することができる。こうした送信データと秘匿鍵の振り分けは、暗号化した送信データD2を伝送路300Bに送出する場合、および暗号化した送信データD3を伝送路300Cに送出する場合についても、同様に行うことができる。

【0074】

このとき、受信側の通信装置203では、別々の伝送路300から送信データD1と秘匿鍵K1が送られてくるが、本体部60は、送信データD1と秘匿鍵K1を対として受け取り、処理すればよいので、その動作が伝送路300の種類や数に影響されることはない。その際、秘匿鍵K1が分割データとなっても、1つのコードに復元することにより、やはり第1の実施の形態と同様に動作することができる。

【0075】

なお、以上は、通信装置103を送信側、通信装置203を受信側として説明したが、逆に通信装置203を送信側、通信装置103を受信側とした場合にも同様の動作を行うようになっている。

【0076】

このように本実施の形態における通信システムは、3つの伝送路300A～300Cに暗号化した送信データと暗号化に用いた秘匿鍵を振り分けて伝送するようにしたので、第1の実施の形態と同様、データ漏洩のリスク軽減の効果を奏すると共に、伝送路選択の幅が広がったことで、その効果を高めることができる。

【0077】

〔第4の実施の形態〕

10

20

30

40

50

上記の各実施の形態では、伝送路 300 のそれぞれが互いに物理的に異なった伝送媒体である場合について説明した。しかしながら、本発明における伝送路は情報を互いに異なる形式で伝送するものであれば足りることから、同種の伝送媒体、もしくは同一の伝送媒体において、互いに適用する通信方式が異なるものや互いに適用する周波数帯が異なるものも、それぞれ独立した伝送経路とみなされる。本実施の形態では、そのような一例として、電力線を用いた通信システムについて説明する。

【0078】

図 15 は、本実施の形態に係る通信システムの構成を表している。ここでは、通信装置 104 と通信装置 204 とが、1つの伝送路 310（電力線）を介して互いに送受信するようになっている。ただし、通信装置 104 は通信制御部 12A、12B、通信装置 204 は通信制御部 22A、22B のそれぞれにおいて、送信データと秘匿鍵を互いに異なる周波数帯域 310A、310B の信号に変換し、それぞれを同一の伝送路 310 に送出するようになっている。

10

【0079】

図 16 は、このうち通信装置 104 の構成を表したものである。なお、通信装置 204 は、対応する構成要素が同様に構成されている。本体部 10 は、第 1 の実施の形態と同様であるが、ここでは、本体部 10 は通信制御部 12A、12B を介在させて伝送路 310 に接続されている。

【0080】

通信制御部 12A、12B のそれぞれは、例えば、AC 用物理層機能部 8B の代わりに AC 用物理層機能部 18A、18B を備えたこと以外は、第 1 の実施の形態における通信制御部 11B と同様の構成となっている。AC 用物理層機能部 18A、18B は、互いに異なる周波数帯域 310A、310B において変復調を行うようになっており、その変調方式には FDM や OFDM 等が適用される。また、AC 用物理層機能部 18A、18B はともに伝送路 310 を媒体とするが、異なる伝送帯域を別々に利用することによって信号の送受信を互いに独立して行うようになっている。

20

【0081】

次に、この通信システムの動作について説明する。図 17 は、本実施の形態における通信システムの通信動作を示すフローチャートである。ここでは、一例として、暗号化した送信データ D1 とその暗号化に用いた秘匿鍵 K1 を、通信装置 104 から通信装置 204 に送信する場合について説明する。

30

【0082】

まず、通信装置 104 の本体部 10 において、送信しようとするデータ D1 を暗号化部 2 が暗号化することにより、秘匿鍵 K1 が生成される（ステップ S21）。次いで、送信データ D1、秘匿鍵 K1 は、メイン CPU 1 に入力され、通信制御部 12A、12B に向けて振り分けられる（ステップ S22）。例えば、周波数帯域 310A は、周波数帯域 310B よりも高周波側にあり、伝送速度も速いものとする、送信データ D1 を周波数帯域 310A に送出するように通信制御部 12A へ出力し、それほどサイズが大きくなることが想定される秘匿鍵 K1 を周波数帯域 310B に送出すべく、通信制御部 12B へ出力することが考えられる。

40

【0083】

メイン CPU 1 から送出された送信データ D1 は、I/O 部 4A を介して通信制御部 12A へ入力され（ステップ S23）、秘匿鍵 K1 は、I/O 部 4B を介して通信制御部 12B へ入力される（ステップ S26）。

【0084】

（変調）

通信制御部 12A では、送信データ D1 を信号に変換する。特に、AC 用物理層機能部 18A において、周波数帯域 310A による変調が施され（ステップ S24）、伝送路 310 に送出される（ステップ S25）。

【0085】

50

一方、通信制御部 12B では、秘匿鍵 K1 が同様に信号に変換される。こちら側では、A/C 用物理層機能部 18B において、周波数帯域 310B による変調が施され（ステップ S27）、伝送路 310 に送出される（ステップ S28）。

【0086】

こうして、それぞれ別々に送出された送信データ D1、秘匿鍵 K1 は、互いに異なる伝送帯域を利用しつつ、同一の媒体である伝送路 310 によって伝送される（ステップ S29）。

【0087】

さらに、送信データ D1 は、通信装置 204 の通信制御部 22A に入力され（ステップ S30）、秘匿鍵 K1 は通信制御部 22B に入力される（ステップ S32）。 10

【0088】

〈復調〉

送信データ D1 は、通信制御部 22A にて、通信制御部 12A で施された過程とは逆の過程を辿ることにより、復調される（ステップ S31）。秘匿鍵 K1 も同様に、通信制御部 22B にて復調される（ステップ S33）。

【0089】

復調された送信データ D1、秘匿鍵 K1 は本体部 20 に入力され、メイン CPU1 を介して復号部 3 に入力される（ステップ S34）。復号部 3 では、秘匿鍵 K1 を用いて送信データ D1 が解読される（ステップ S35）。 20

【0090】

なお、以上の動作は、通信装置 204 から通信装置 104 へデータを送信する場合であっても同様に行うことができる。また、本実施の形態では、1つの伝送路 310 を用いるようにしたが、これは、通常の電力線が 2重に敷設されていないことによる。ただし、電力線が 2重（またはそれ以上）に敷設されている場所においてはその限りではなく、2つ（以上）の電力線を利用し、それぞれに異なる伝送帯域を割り当てるようにしてもよい。さらに、秘匿鍵を、2つ以上の周波数帯に分割して伝送することもできる。なお、このように送信データと秘匿鍵を異なる周波数帯域を利用して伝送する例としては、電力線通信のほかに無線通信が挙げられる。

【0091】

このように本実施の形態では、送信データと秘匿鍵を、変調帯域が異なることにより区別される経路により伝送するようにしたので、同種の伝送媒体や単一の伝送媒体においても、送信データと秘匿鍵の両方を傍受などによって不正に取得される可能性が低くなる。よって、こうした方法によっても、第1の実施の形態と同様の効果を奏することができる。 30

【0092】

なお、本発明は、上記実施の形態および変形例に限定されず、種々の変形実施が可能である。例えば、上記実施の形態では、送信データは暗号化によって秘匿されるようにしたが、第3者に対し秘密にする手段であればよく、例えば暗号化以外にパスワードなどを用いて秘匿化することができる。この場合、パスワードが秘匿鍵に相応し、パスワードには、装置に割り振られた IP アドレスや MAC アドレスを使うことができる。

【0093】

また、上記実施の形態では、送受信を行う2つの通信装置間における伝送路は2つまたは3つとした場合について説明したが、これに限らず、3つ以上の伝送路が多重に併設されていてもよい。こうすることによって、より多くの伝送路に秘匿鍵を分割して伝送することができ、またデータ振り分けの自由度が高くなるために、データの安全性を高めることができる。 40

【0094】

また、各実施の形態においては、伝送路 300、310 で接続された2つの通信装置を双方とも送受信できるようにしたが、実際のネットワークの態様に合わせ、少なくともいずれか一方が送信機または受信機（例えばプリンタである場合など）としてのみ機能する機器としても構わない。 50

【0095】

これに関連して、本発明は、通信装置の接続形態を1対1に限定するものではなく、取り得るいろいろな態様（バス型、スター型など）において適宜に適用することができる。図18は、そうした構成の簡単な具体例を示している。通信装置121、122、123は、伝送路320A、320Bによって接続されている。伝送路320A、320Bは、LANケーブル、電力線、無線等どのような種類の媒体であってもよい。その接続関係は、通信装置121に通信装置122、123が接続された1対多対応である場合もあるし、3者が相互に接続されている場合もある。いずれにしても、伝送路320A、320Bを利用して、送信データと秘匿鍵とを振り分けて伝送することが可能となっている。さらに、通信装置140のように、単一の伝送路141によってネットワークに接続されているために、データを振り分けて伝送することができない機器も、適宜に存在していて構わない。

10

【0096】

また、こうしたネットワークを構築するにあたり、上記の各実施の形態を組み合わせる適用するようにしてもよい。なお、第2ないし第4の実施の形態に対し、第1の実施の形態における2つの変形例を適宜応用することもできる。

【0097】

さらに、第4の実施の形態においては、変調周波数帯域が異なる場合について説明したが、そのほかにも、同種または同一の伝送媒体を用いる場合に利用できる互いに異なる信号変換方式として、互いに異なる通信方式を利用する場合が挙げられる。具体的には、SS通信方式（Spread Spectrum Communication：スペクトラム拡散方式）とOFDM方式を併用することが考えられる。前者は、盗聴が難しく、機密保護に優れ、後者は伝送速度が高いという特徴がある。そこで、前者を秘匿鍵の伝送に用い、後者を送信データの伝送に用いるとよい。

20

【0098】

【発明の効果】

以上説明したように、本発明の第1の観点に係る送信機によれば、秘匿鍵を用いて秘匿化した送信データを複数の伝送路のうちの1の伝送路を経由して受信機に送信すると共に、秘匿鍵を複数の伝送路のうちの他の伝送路を経由して受信機に送信するようにしたので、送信データと秘匿鍵とは互いに異なる伝送路により別々に伝送され、両方が同時に傍受されるおそれが減る。したがって、データ漏洩のリスクが軽減され、通信情報の秘密保護を強化することが可能となる。

30

【0099】

また、本発明の第2の観点に係る送信機によれば、互いに異なる周波数帯の複数の搬送波を利用して受信機との間で通信を行う送信機であって、秘匿鍵を用いて秘匿化した送信データを複数の搬送波のうちの1の搬送波を用いて受信機に送信すると共に、秘匿鍵を複数の搬送波のうちの他の搬送波を用いて受信機に送信するようにしたので、送信データと秘匿鍵とが、互いに異なる周波数帯において別個独立して伝送され、両方が同時に傍受されるおそれが減る。よって、この場合も、通信情報の秘密保護を強化することが可能である。

40

【0100】

本発明の第1の観点に係る受信機によれば、秘匿鍵を用いて秘匿化された送信データを、複数の伝送路のうちの1の伝送路を経由して送信機から受信すると共に、秘匿鍵を、複数の伝送路のうちの他の伝送路を経由して送信機から受信するようにしたので、本発明の第1の観点に係る送信機との間で、秘匿鍵とこの秘匿鍵を使って秘匿化した送信データとを互いに異なる伝送路に伝送する方式による通信を可能とする。

【0101】

なお、本発明の第2の観点に係る受信機によれば、秘匿鍵を用いて秘匿化され、複数の搬送波のうちの1の搬送波を用いて送信機から送信された送信データを受信すると共に、複数の搬送波のうちの他の搬送波を用いて送信機から送信された秘匿鍵を受信するようにし

50

たので、本発明の第2の観点に係る送信機との間で秘匿鍵とこの秘匿鍵を使って秘匿化した送信データとを互いに異なる伝送帯域に伝送する方式での通信を可能とする。

【0102】

さらに、本発明による通信システム、および本発明による通信方法によれば、送信機は、秘匿鍵を用いて秘匿化した送信データを複数の伝送路のうちの1の伝送路を経由して受信機に送信すると共に、秘匿鍵を複数の伝送路のうちの他の伝送路を経由して受信機に送信し、受信機は、秘匿鍵を用いて秘匿化された送信データを1の伝送路を経由して受信すると共に、秘匿鍵を他の伝送路を経由して受信するようにしたので、秘匿鍵とこの秘匿鍵を使って秘匿化した送信データとを互いに異なる伝送路に伝送する方式での通信を実現することができる。

10

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係る通信システムの構成図である。

【図2】図1に示した通信装置の構成を表すブロック図である。

【図3】図1に示した通信システムにおける基本的なデータ送受信方法を説明するための図である。

【図4】図1に示した通信システムにおける通信動作を示すフローチャートである。

【図5】図1に示した通信システムの通信動作を示すタイミングチャートである。

【図6】図1に示した通信システムにおけるデータフローブロックである。

【図7】図1に示した通信システムの第1の変形例におけるシステム構成を表す図である。

20

【図8】図7に示した通信システムの通信動作を示すタイミングチャートである。

【図9】図7に示した通信システムにおけるデータフローブロックである。

【図10】図1に示した通信システムの第2の変形例におけるシステム構成を表す図である。

【図11】図10に示した通信装置の構成を表すブロック図である。

【図12】第2の実施の形態に係る通信システムの構成図である。

【図13】図12に示した無線用の通信制御部の構成を表すブロック図である。

【図14】第3の実施の形態に係る通信システムの構成図である。

【図15】第4の実施の形態に係る通信システムの構成図である。

【図16】図15に示した通信装置の構成を表すブロック図である。

30

【図17】図15に示した通信システムの通信動作を示すフローチャートである。

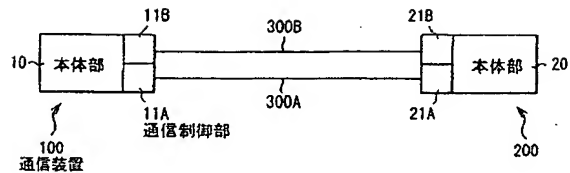
【図18】本発明の通信システムの一具体例を表す図である。

【符号の説明】

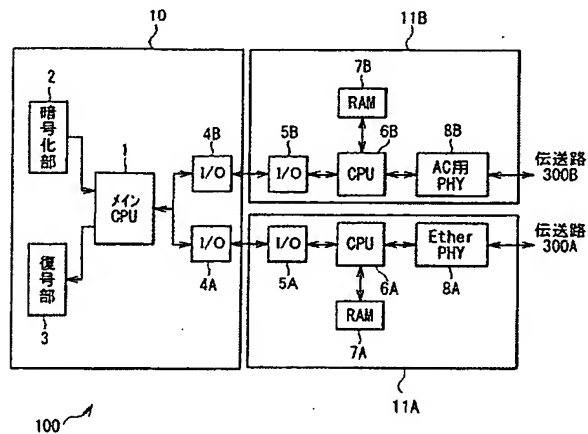
1…メインCPU、2…暗号化部、3…復号部、4A, 4B…I/O部（本体部側）5, 5A～5C…I/O部（通信制御部側）、6A～6C…CPU、7A～7C…RAM、8A…イーサネット（R）物理層機能部、8B, 18A, 18B…AC用物理層機能部、8C…無線用物理層機能部、10, 20, 30, 40, 50, 60…本体部、11, 11A～11C, 12A, 12B, 21, 21A～21C, 22A, 22B…通信制御部、100～104, 121～123, 200～204…通信装置、300, 300A～300C, 310, 320A, 320B…伝送路、310A, 310B…周波数帯域、D1, D2…送信データ、K1, K2…秘匿鍵

40

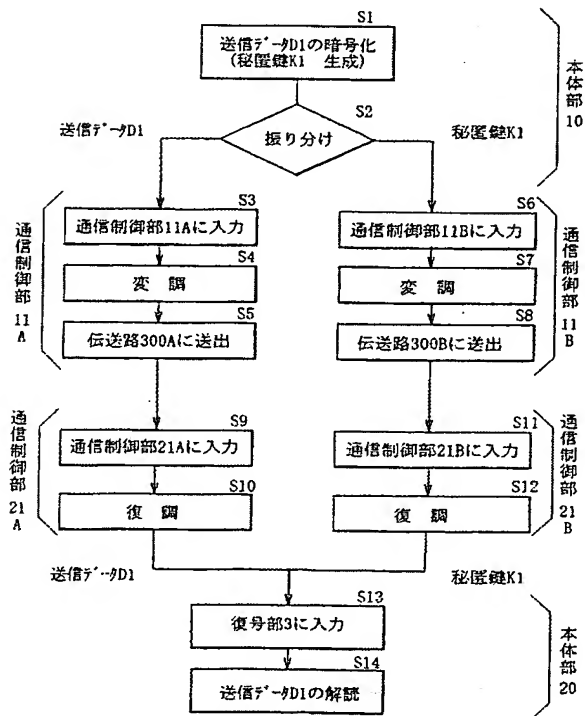
【図1】



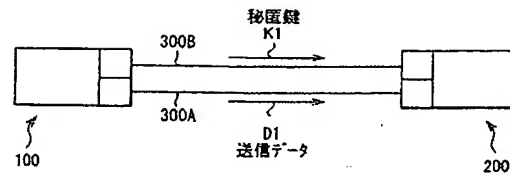
【図2】



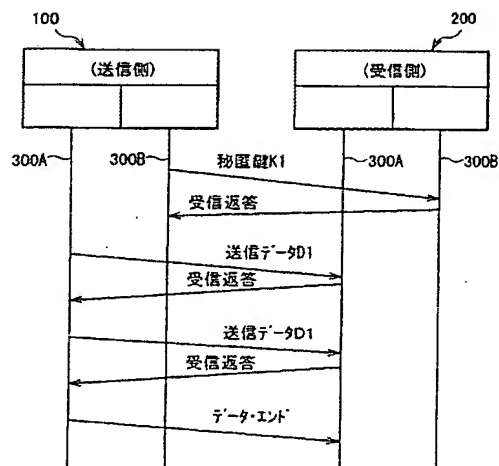
【図4】



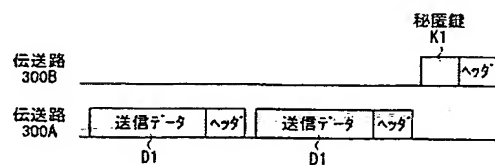
【図3】



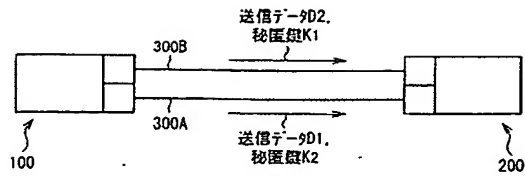
【図5】



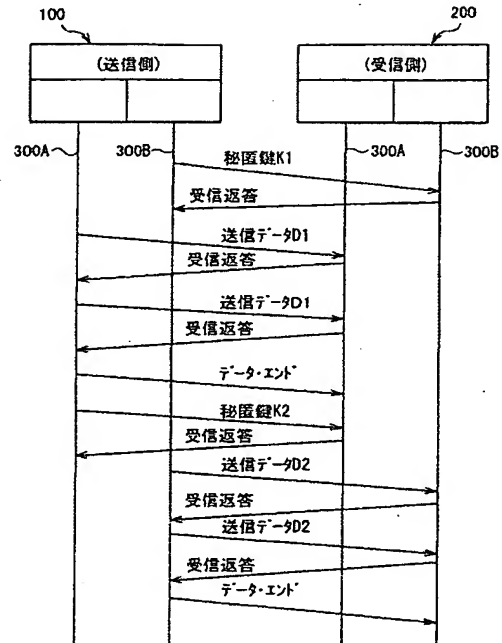
【図6】



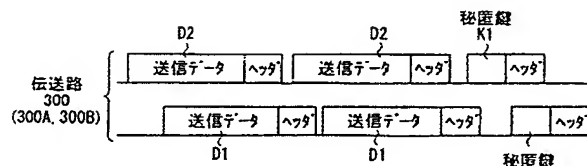
【図7】



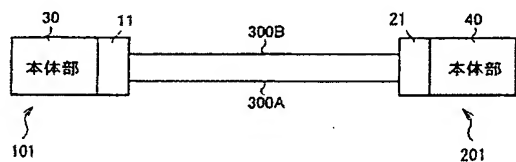
【図8】



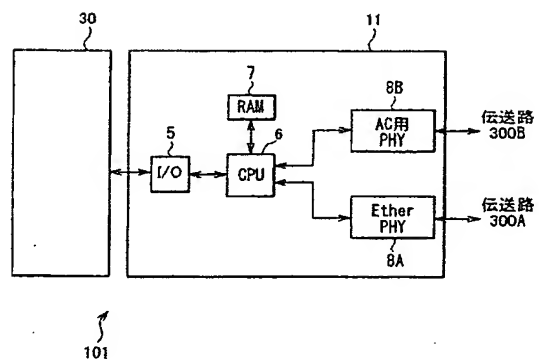
【図9】



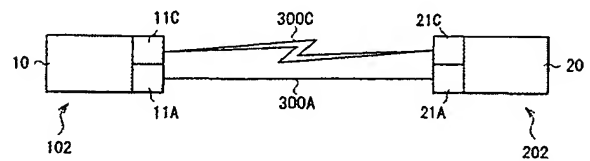
【図10】



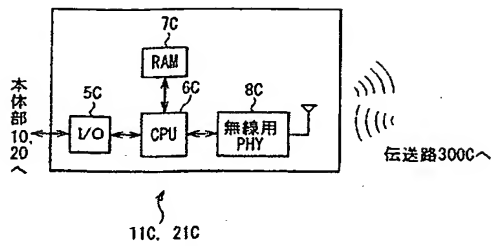
【図11】



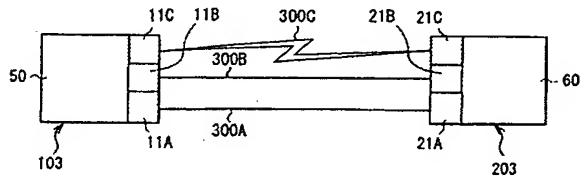
【図12】



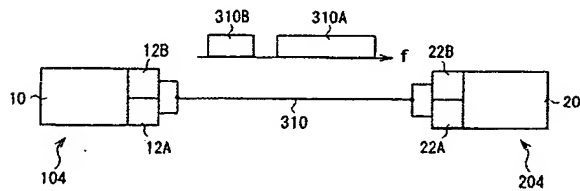
【図13】



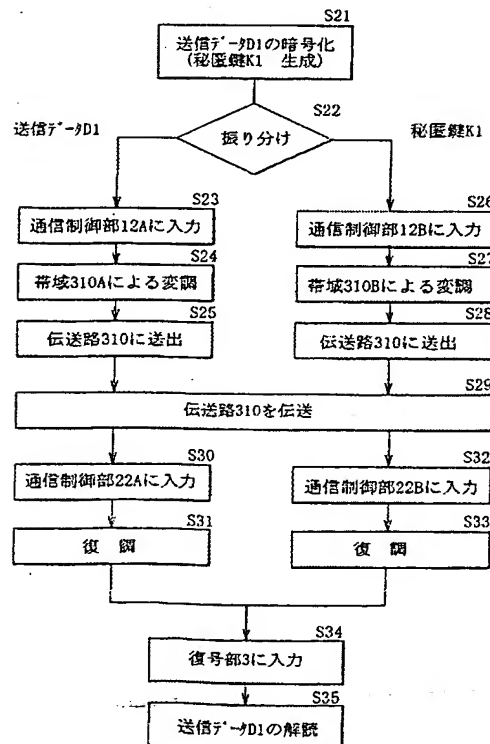
【図14】



【図15】



【図17】



【図18】

